AMENDMENTS TO THE CLAIMS

1. (Currently amended) A security and filtering software embodied in a non-transitory computer-readable medium, the software comprising:

(a) an administrative module that a user interacts with for creating user accounts and configuring those user accounts,

the administrative module for accepting user inputs for configuration settings for inbound communications, for outbound communications or for inbound and outbound communications,

(b) a domain filtering engine, capable of one of

(i) both (I) using a friendly outbound list and an unfriendly outbound list, only one of which is active at any given time and (II) using a friendly inbound list and an unfriendly inbound list, only one of which is active at any given time; and

(ii) using a friendly inbound list and an unfriendly inbound list, only one of which is active at any given time,

~~either capable of using a friendly outbound list and an unfriendly outbound list only one of which is active at any given time and such that use of one outbound list is independent of an outcome of use of the other outbound list or capable of using a friendly inbound list and an unfriendly inbound list in any order and such that use of one inbound list is independent of an outcome of use of the other inbound list, only one of which is inbound list being active at any given time or capable of both using a friendly outbound list and an unfriendly outbound list only one of which is active at any given time and such that use of one outbound list is independent of the outcome of use of the other outbound list and using a friendly inbound list and an unfriendly inbound list in any order and such that use of one inbound list is independent of the outcome of use of the other inbound list, only one inbound list being of which is active at any given time the~~

~~friendly outbound list, the unfriendly outbound list,~~ the friendly inbound list, the unfriendly inbound list, being uniquely configured for each user account,

the using of the friendly or unfriendly outbound lists by the domain filtering engine involving checking user requested web resources against the friendly or unfriendly outbound lists, the using of the friendly or unfriendly inbound lists by the domain filtering engine involving -checking the identity of a requesting client against the friendly or unfriendly inbound lists, the "requesting client" is at least one of (i) an HTTP (Hypertext Transfer Protocol) client and (ii) a web browser.

2. (original) The software of claim 1, wherein the domain filtering engine also has an optional alert system for hard filtering, for soft filtering or for both hard and soft filtering.

3. (Currently amended) The software -of claim 1, wherein the domain filtering engine has an outbound privacy shield for blocking disapproved ~~character~~ strings representing confidential information without blocking ~~character~~ strings that do not represent confidential information.

4. (canceled)

5. (canceled)

6. (Previously presented) The software of claim 1, including an automated scheduler that controls a launching of the software automatically and decides which user account to activate and when to shut off an access to a world wide web.

7. (canceled)

8. (canceled)

9. (Currently amended) The software of claim 1, wherein the administrative module includes an editor, the editor including an editing pane, said editor also including an encryption function, said encryption function capable of encrypting all of an e-mail message and capable of encrypting only a portion of the e-mail message, the portion being less than the entire e-mail message, the portion selected by the user.

10. (Currently amended) The software of claim 1, wherein the domain filtering further includes an application server acting (i) internally, (ii) externally or (iii) internally and externally to communicate with the domain filtering engine and acting externally as a proxy server that receives requests from ~~HTTP~~ "requesting clients", forwards the requests to servers, receives a server response and forwards the server response to the ~~HTTP~~ "requesting clients".

11. (Original) The software of claim 1, wherein the administrative module is also capable of configuring an automated configuration script file for accessing the global

telecommunications network.

12. (Currently amended) The software ~~-~~of claim 1, further comprising ~~wherein for e-mail filtering includes~~ at least one of (i) an option of hard e-mail filtering in which an incoming e-mail is deleted from a user e-mail inbox and (ii) an option for soft filtering in which an incoming e-mail remains in the user e-mail inbox but is inaccessible to the user.

13. (Currently amended) The software of claim 1, further including

a content filtering engine capable of performing content filtering including checking a content of a requested document against a friendly content inbound list~~,~~ and against an unfriendly content inbound list, only one of the friendly content inbound list and the unfriendly content inbound list being active at any given time~~, the checking of one content inbound list independent of an outcome of a checking of the other inbound content list~~, the friendly content inbound list and the unfriendly content inbound list being uniquely configured for each user account, and

(i) if the content filtering involves- hard filtering then

against the unfriendly content inbound list either (a) passing the requested document if the said content of the requested document is not on the unfriendly content inbound list or (b)-rejecting the requested document if the said content of the requested document is on the unfriendly content inbound list and

~~for hard filtering~~ against the friendly content inbound list either (a) passing the requested document if the said content of the requested document is on the friendly

content inbound list or (b) rejecting the requested document if the said content of the requested document is not on the friendly content inbound list and

(ii) if the content involves -soft filtering then

against the unfriendly content inbound list either (a) approving the content of the requested document and passing the requested document if the said content is not on the unfriendly content inbound list or (b) rejecting the content of the requested document and passing a remainder of the requested document if the said content is on the unfriendly content inbound list and

-against the friendly content inbound list either (a) rejecting the requested document if parts of the content is not on the friendly content inbound list or (b) passing the requested document if the said content is on the friendly content inbound list.

14. (Currently amended) A security and filtering software embodied in a non-transitory computer-readable medium, the software, comprising:

(a) an administrative module that a user interacts with for creating user accounts and configuring those user accounts,

the administrative module for accepting user inputs for configuration settings for inbound communications, outbound communications or inbound and outbound communications

(b) a content filtering engine capable of performing content filtering including checking, during a web server response to a request for a web resource, a content of a requested document against a friendly content inbound list, and against an unfriendly content inbound list ~~in any order, a checking of the content of one of the content inbound~~

~~lists independent of an outcome of a checking of the content of the other content inbound list~~, only one of the friendly content inbound list and the unfriendly content inbound list being active ~~for a~~ at any given time ~~request by a client~~, the friendly content inbound list and the unfriendly content inbound list being uniquely configured for each user account, and

(i) if the content filtering involves hard filtering then

against the unfriendly content inbound list either (a) passing the requested document if the said content of the requested document is not on the unfriendly content inbound list or (ii) rejecting the requested document if the said content of the requested document is on the unfriendly content inbound list and

against the friendly content inbound list either (a) passing the requested document if the said content of the requested document is on the friendly content inbound list or (b) rejecting the requested document if the said content of the requested document is not on the friendly content inbound list and

(ii) if the content filtering involves soft filtering then

against the unfriendly content inbound list either (a) approving the content of the requested document and passing the requested document if the said content is not on the unfriendly content inbound list or (b) rejecting the content of the requested document and passing a remainder of the requested document if the said content is on the unfriendly content inbound list and

against the friendly content inbound list either (a) rejecting the requested document if the said content is not on the friendly content inbound list or (b) passing the requested document if the said content is on the friendly content inbound list.

the software configured to perform the content filtering, including the checking, independent of whether the software has performed domain filtering.

15. (canceled)

16. (canceled)

17. (previously presented) The software of claim 14, wherein the content filtering engine has an inbound privacy shield for blocking scripting language functions for particular user accounts.

18. (Previously presented) The software of claim 13, wherein the content filtering engine, when performing at least one of soft filtering and hard filtering, can also replace a requested document that has been rejected with a replacement document selected by a user of the administrator account.

19. (Currently amended) The software of claim 1, wherein the domain filtering also includes with respect to both inbound and outbound requests for hard filtering three alternative paths, namely ~~either~~ (i) approving the request, (ii) terminating the request and (iii) ~~or~~ terminating and re-routing the request

20. (Currently amended) The software of claim 1, wherein the domain filtering also includes with respect to both inbound and outbound requests for soft filtering

passing disapproved requests ~~and sending an alert to authorized recipients regarding the disapproved request~~.

21. (Currently amended) The software of claim 19, wherein the domain filtering also provides that, for requests that are terminated and re-rerouted, inbound communications are arranged so that an actual location of a highly sensitive resource is located in an unpublished location that is a replacement location and~~, to which~~ requests rejected by the software are rerouted,
wherein clients of approved users are listed in the application server in the unfriendly inbound list and are sent by the application server to the replacement location, and wherein clients of unapproved users are not listed in the unfriendly inbound list and have their request sent to a published address that contains harmless information.

22. (Canceled)

23. (Currently amended) The software of claim 1, wherein the domain filtering engine is capable of using from the administrative module a domain outbound exception list of web resources, is capable of using from the administrative module a domain inbound exception list of client identity information~~web resources~~ and is capable of using from the administrative module a domain outbound exception list of web resources and a domain inbound exception list of client identity information~~web resources~~, the domain outbound exception list and the domain inbound exception list being uniquely configured for each user account.

24. (Currently amended) The software of claim 1, wherein regarding ~~the~~ domain filtering, further comprising for soft filtering ~~involves~~ passing disapproved requests and sending an e-mail alert to authorized recipients regarding the disapproved request.

25. (Currently amended) The software of claim 1, said administrative module having list maintenance functions including list editing, list deleting, searching of lists, saving of lists, adding and deleting users~~, and having list maintenance functions including list editing, interchanging lists and importing and exporting lists~~.

26. (previously presented) The software of claim 25, said administrative module having proxy chaining functions including proxy chaining routing.

27. (Currently amended) The software of claim 1, said administrative module able to configure a range of access levels and being capable of creating three types of user accounts that have unique authentication credentials for each user account including (a) an administrator account that is self-configuring and that controls automated services and selects for each account hard filtering or soft filtering, (b) regular accounts with administrative privileges other than a~~the~~ privilege to create additional accounts, view information on any other accounts or configure automated services and (c) regular accounts without administrative privileges.

28. (Currently amended) The software of claim 27~~1~~, said administrative module

able to create four types of user accounts -including a fourth type of user account namely one anonymous guest user account to be used by general users who have no authentication credentials.

29. (Currently amended) The software of claim 1, wherein the administrative module is capable of creating, modifying ~~or~~and reading the configuration settings ~~or~~and is capable of storing the configurations settings in memory, cache, encrypted files, plain text files, storage devices, computer storage media or as web resources.

30. (Previously presented) The software of claim 27, wherein the administrative module is capable of at least one of (i) configuring the range of access levels for the user accounts created and (ii) configuring automated services.

31. (Previously presented) The software of claim 1, wherein the administrative module is capable of configuring at least one of (i) automated services and (ii) user account configurations.

32. (Currently amended) The software of claim 23, wherein the domain filtering engine is capable of performing domain filtering, said domain filtering including checking the identity of a requesting client against at least one of the friendly inbound list and the~~or~~ unfriendly inbound list and against the domain inbound exception list ~~and including for outbound web-based resource requests either~~

~~(i) checking user requested applications or~~

~~(ii) checking user requested domains or~~

~~(iii) checking user requested URLs or~~

~~(iv) checking user requested addresses or~~

~~(v) checking user requested links~~

~~against the friendly outbound list and/or the unfriendly outbound list and outbound exception list and then with respect to both inbound and outbound client communication requests for hard filtering unless overruled by the outbound exception list or domain inbound exception list either approving the request, terminating the request or terminating and re-routing the request.~~

33. (Previously presented) The software of claim 23, the soft domain filtering engine capable of performing domain filtering and for soft domain filtering unless overruled by the outbound exception list or domain inbound exception list passing disapproved requests and sending an alert to authorized recipients regarding the disapproved request.

34. (previously presented) The software of claim 33, wherein the soft domain filtering engine, for soft filtering, passes disapproved requests and sends alerts to authorized recipients regarding the disapproved requests.

35. (Previously presented) The software of claim 27, wherein the software is programmed to check an identity of a user who logs in and who presents a unique

authentication credential prior to checking an identity of at least one of (i) a requesting client and (ii) a requested resource.

36. (Previously presented) The software of claim 35, wherein the software is also programmed, upon a successful authentication of the user's credential, to use a configuration of the user's account to check the identity of at least one of (i) the requesting client and (ii) the requested resource.

37. (Currently amended) The software of claim 35, wherein the software is also programmed that if the software fails to authenticate the user, the ~~first proxy server~~ domain filtering engine offers that user an opportunity to log in as an anonymous guest user.

38. (previously presented) The software of claim 1, wherein the computer-readable medium is in a computer.

39. (previously presented) The software of claim 1, wherein the computer-readable medium is in hardware.

40. (Currently amended) The software ~~-~~of claim 13, further comprising ~~wherein for e-mail filtering includes~~ an option of hard e-mail filtering in which an incoming e-mail is deleted from a user e-mail inbox.

41. (Currently amended) The software ~~of~~ claim 13, further comprising~~wherein for e-mail filtering includes~~ an option of soft filtering in which an incoming e-mail remains in the user e-mail inbox but is inaccessible to the user.

42. (Currently amended) The software of claim 13, wherein the content filtering engine is capable of using from the administrative module at least one of the following

(a) an unfriendly hard content exception list;

(b) ~~and/or~~ a friendly hard content exception list;

(c)~~and/or~~ an unfriendly soft content exception list; and

(d) ~~and/or~~ a friendly soft content exception list,

each of the unfriendly soft content exception list, ~~and a~~ friendly soft content exception list, ~~and~~ unfriendly hard content exception list and ~~the~~ friendly hard content exception list, being uniquely configured for each user account.

43. (Currently amended) The software ~~of~~ claim 42, wherein the content filtering engine is capable for hard filtering

against a friendly hard content inbound list, an unfriendly hard content inbound list, a friendly hard content exception list and an unfriendly hard content exception list,

~~the friendly content inbound list, the unfriendly content inbound list,~~ only one of the friendly content inbound list and the unfriendly content inbound list being active at any given time, and ~~then for hard filtering~~

against the unfriendly content inbound list either (a) passing the requested document if the said content of the requested document is not on the unfriendly content

inbound list or (b) unless overruled by the unfriendly hard content exception list rejecting the requested document if the said content of the requested document is on the unfriendly content inbound list and

~~then for hard filtering~~ against the friendly content inbound list either (a) unless overruled by the friendly hard content exception list passing the requested document if the said content of the requested document is on the friendly content inbound list or (b) rejecting the requested document if the said content of the requested document is not on the friendly content inbound list.

44. (Currently amended) The software ~~-~~of claim 42, wherein the content filtering engine is capable for soft filtering doing at least one of the following:

against the unfriendly content inbound list either (a) unless overruled by the unfriendly soft content exception list approving the content of the requested document and passing the requested document if the said content is not on the unfriendly content inbound list or (b) unless overruled by the unfriendly soft content exception list rejecting the content of the requested document and passing a remainder of the requested document if the said content is on the unfriendly content inbound list~~,-and/or~~

~~for soft filtering~~ against the friendly content inbound list either (a) unless overruled by the friendly soft content exception list rejecting the requested document if the said content is not on the friendly content inbound list or (b) unless overruled by the friendly soft content exception list passing the requested document if the said content is on the friendly content inbound list.

45. (Currently amended) The software ~~-~~of claim 13, further comprising~~wherein~~ a content filtering engine capable of using from the administrative module a soft content exception list~~,~~ and ~~using~~ a hard content exception list, the soft content exception list~~,~~ and hard content exception list ~~are~~ being uniquely configured for each user account.

46. (Currently amended) The software of claim 14, wherein the content filtering engine, when performing at least one of (i) hard filtering and (ii) soft filtering, is also capable of replacing~~able to replace~~ a requested document that has been rejected, with a replacement document selected by a user of the administrator account.

47. (Currently amended) The software ~~-~~of claim 14, said content filtering also including e-mail filtering that checks at least one of

(i) a subject,

(ii) a sender's address and

(iii) a sender's domain

against at least one of (a) an unfriendly e-mail list~~,~~ and (b) a friendly e-mail list.

48. (Currently amended) The software of claim 14, wherein the content filtering engine is capable of using from the administrative module an e-mail exception list, the e-mail exception list being uniquely configured for each user account.

49. (previously presented) The software of claim 48, said content filtering also including e-mail filtering that checks a subject, a sender's address and a sender's domain

against an unfriendly e-mail list, a friendly e-mail list and an e-mail exception list.

50. (Currently amended) The software of claim 14, wherein the software is programmed to check an identity of a user who logs in and who presents a unique authentication credential prior to the software checking an identity of at least one of (i) a requesting client and (ii) a requested resource, the "requesting client" is at least one of (i) an HTTP (Hypertext Transfer Protocol) client and (ii) a web browser.

51. (Previously presented) The software of claim 50, wherein the software is also programmed, upon a successful authentication of the user's credential, to use a configuration of the user's account to check the identity of at least one of (i) the requesting client and (ii) the requested resource.

52. (Currently amended) The software of claim 50, wherein the software is also programmed that if the software fails to authenticate the user, the domain filtering engine~~first proxy server~~ offers that user an opportunity to log in as an anonymous guest user.

53. (Previously presented) The software of claim 14, wherein the computer-readable medium is in a computer.

54. (Previously presented) The software of claim 14, wherein the computer-readable medium is in hardware.

55. (Previously presented) The software of claim 1, includes an automated list updater that updates the friendly inbound list, the unfriendly inbound list, the friendly outbound list and the unfriendly outbound lists for each user account from links on the web.

56. (Previously presented) The software of claim 9, wherein the encryption function generates one or more secret symmetric encryption keys, the one or more encryption keys being uniquely associated with a text presented by a user of the editing pane.

57. (Currently amended) A security and filtering software embodied in a non-transitory computer-readable medium, the software comprising:

(a) an administrative module that a user interacts with for creating user accounts and configuring those user accounts,

the administrative module for accepting user inputs for configuration settings for inbound communications, for outbound communications or for inbound and outbound communications,

(b) a domain filtering engine, capable of one of

(i) both (I) using a friendly outbound list and an unfriendly outbound list, only one of which is active at any given time and (II) using a friendly inbound list and an unfriendly inbound list, only one of which is active at any given time; and

(ii) using a friendly inbound list and an unfriendly inbound list, only one

of which is active at any given time,

~~either capable of using a friendly outbound list and an unfriendly outbound list only one of which is active at any given time and such that use of one outbound list is independent of an outcome of use of the other outbound list or capable of using a friendly inbound list and an unfriendly inbound list in any order and such that use of one inbound list is independent of an outcome of use of the other inbound list, only one inbound list being active at any given time or capable of both using a friendly outbound list and an unfriendly outbound list only one of which is active at any given time and such that use of one outbound list is independent of the outcome of use of the other outbound list and using a friendly inbound list and an unfriendly inbound list in any order and such that use of one inbound list is independent of the outcome of use of the other inbound list, only one inbound list being active at any given time~~ the friendly outbound list, the unfriendly outbound list, the friendly inbound list, the unfriendly inbound list, being uniquely configured for each user account,

the using of the friendly or unfriendly outbound lists by the domain filtering engine involving checking user requested web resources against the friendly or unfriendly outbound lists, the using of the friendly or unfriendly inbound lists by the domain filtering engine involving checking the identity of a requesting client against the friendly or unfriendly inbound lists, the "requesting client" is at least one of (i) an HTTP (Hypertext Transfer Protocol) client and (ii) a web browser,

wherein the domain filtering further includes an application server acting (i) internally, (ii) externally or (iii) internally and externally, to communicate with the domain filtering engine and

wherein the application server acts externally within a deployment of a chain of proxy servers including at least a first proxy server that receives requests from ~~HTTP~~ "requesting clients" and either (i) forwards the requests to a last proxy server, or (if) there are is an intermediate proxy server, forwards the requests through one~~a zero~~ or more intermediary proxy servers to the~~a~~ last proxy server,

said last proxy server forwarding the requests to servers, and

wherein the last proxy server receives a server response and forwards the server response either (a) back to the first proxy server or (b) if there are intermediate proxy servers through the ~~zero~~one or more intermediary proxy servers back to the first proxy server, and wherein the~~which~~ first proxy server forwards the server response to ~~HTTP~~ "requesting clients".

58. (New) The software of claim 10, wherein the application server, instead of acting externally as a first proxy server, acts externally within a deployment of a chain of proxy servers including at least a first proxy server that receives requests from "requesting clients" and either (i) forwards the requests to a last proxy server, or (if) there are is an intermediate proxy server, forwards the requests through one or more intermediary proxy servers to the last proxy server,

said last proxy server forwarding the requests to servers, and

wherein the last proxy server receives a server response and forwards the server response either (a) back to the first proxy server or (b) if there are intermediate proxy servers through the one or more intermediary proxy servers back to the first proxy server, and wherein the first proxy server forwards the server response to "requesting clients".